UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/862,888	05/21/2001	Kiyoko Katayanagi	81942.0015	9843

26021 7590 03/25/2005		

HOGAN & HARTSON L.L.P.
500 S. GRAND AVENUE
SUITE 1900
LOS ANGELES, CA 90071-2611

EXAMINER
AKPATI, ODAICHE T

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

		Application No.	Applicant(s)
Office Action Summary		09/862,888	KATAYANAGI ET AL.
		Examiner	Art Unit
		Tracey Akpati	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☐ This action is **FINAL.**   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-38* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-38* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 May 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☒ All   b)☐ Some * c)☐ None of:

      1.☒ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____ .

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
        application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date *5/21/01*.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____ .

DETAILED ACTION

Drawings

New corrected drawings in compliance with 37 CFR 1.121(d) are required in this

application because Fig. 1 has the same reference number used to a different element of the

figure e.g. C and x. Applicant is advised to employ the services of a competent patent

draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new

drawings. The corrected drawings are required in reply to the Office action to avoid

abandonment of the application. The requirement for corrected drawings will not be held in

abeyance.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or
> any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
> requirements of this title.

The claimed invention is directed to non-statutory subject matter. With respect to claims 1, 4, 6,

9, 11 and 15, the examiner respectfully asserts that the subject matter specified in the claims does

not fall within the statutory classes listed in 35 USC 101. Claims 1, 4, 6, 9, 11 and 15 are

rejected as being directed to an abstract idea with no practical information.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-6, 8-11, 13-21, 23-26, 28-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kasahara et al (6798884 B1).

With respect to Claim 1, the limitation of "creating a composite vector by adding a random number vector whose components are a plurality of arbitrarily selected random numbers to a plaintext vector having a plurality of components obtained by dividing a plaintext to be encrypted and obtaining a ciphertext by using the created composite vector and a publicized public vector" is met on column 2, lines 38-52; column 3, lines 7-26; column 8, lines 66-67; column 9, lines 1-26. The message vector represents the composite vector. The random number vector, v represents the random number vector, the ciphertext, C represents the ciphertext and the public key vector, c represents the publicized public vector.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have the message vector represent the composite vector because the message vector, m is derived by combining a random number vector and a plaintext vector. The plaintext vector is composed of a plurality of components obtained by dividing the plaintext message (column 2, 38-46) by K. Hence it would have been obvious to add the random number vector to a plaintext vector to create the composite vector because adding vectors is a form of combining vectors.

With respect to Claim 2, the limitation of "wherein a result of product-sum operation of the components of said composite vector and the components of said public vector is made the ciphertext" is met on column 9, lines 24-26. The message vector, m represents the composite

vector. The product-sum operation is defined in the applicant's specification on page 3 as an encryption scheme in which one entity creates a ciphertext using a plaintext vector obtained by dividing the plaintext into k parts.... This has already been met by Claim 1 rejection.

With respect to Claim 3, the limitation of "wherein a remainder formed by dividing a result of product-sum operation of the components of said composite vector and the components of said public vector by a modulus is made the ciphertext" is met on column 9, lines 16-23.

With respect to Claim 4, the limitation of "creating a third vector having (k+n) components by adding a second vector whose components are n arbitrarily selected random numbers to a first vector having k components obtained by dividing a plaintext to be encrypted into k parts and obtaining a ciphertext by using the created third vector and a fourth vector whose (k+n) components $Di(1 \leq i \leq k+n)$ are respectively set such that $Di = d/di$ (where $d = d1d2...dk+n$) by using an integer di" is met on column 2, lines 38-52. Di represents the third vector, n being equal to -1, d represents the first vector and the base vector, D represents the fourth vector.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have a third vector with k+n components because in the reference on column 2, Di maximum value is K-1. This is the same linear graph as k+n but with n = -1.

With respect to Claims 5, 8, 10, 14, the limitation of "wherein the ciphertext is obtained based on a product-sum operation of the components of said third vector and components of a

public-key vector modulo transformed based on said fourth vector" is met on column 2, lines 47-62; column 3, lines 6-26.

With respect to Claim 6, the limitation of "creating a third vector having (k+n) components by adding a second vector whose components are n arbitrarily selected random numbers to a first vector having k components obtained by dividing a plaintext to be encrypted into k parts and obtaining a ciphertext by using the created third vector and a fourth vector whose (k+n) components Vi($1 \leq i \leq k+n$) are respectively set such that Vi= (d/di).vi (where d = did2...dk+n) by using an integer di" is met on column 2, lines 53-65. Di in the reference represents Vi because it is a vector within the same range with the lower threshold value being equal to 0 instead of 1.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have a fourth vector with k+n components because in the reference on column 2, Di maximum value is K-1. This is the same linear graph as k+n but with n = -1.

With respect to Claim 9, the limitation of "creating a third vector having (k+n) components by adding a second vector whose components are n arbitrarily selected random numbers to a first vector having k components obtained by dividing a plaintext to be encrypted into k parts and obtaining a ciphertext by using the created third vector and L sets (L$\geq$2)of fourth vector whose (k+n) components $Di^{(y)}$ ($1 \leq I \leq k+n$, $1 \leq y \leq L$) are respectively set such that $Di^{(y)} = d^{(y)}/di^{(y)}$ (where $d^{(y)} = d_1^{(y)} d_2^{(y)} ... d_{k+n}^{(y)}$) in each set by using L sets of integers $di^{(y)}$" is met on column 2, lines 38-52; column 10, lines 36-67; and column 11, lines 1-11.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have a fourth vector with a second variable of y so as to include an additional factor into the cryptographic system. This is the equivalent of extending a two-dimensional graph to a three dimensional one by adding on a z-axis so as to further detail the specification.

With respect to Claim 11, the limitation of "creating a third vector having (k+n) components by adding a second vector whose components are n arbitrarily selected random numbers to a first vector having k components obtained by dividing a plaintext to be encrypted into k parts and obtaining a ciphertext by using the created third vector and L sets ($L \geq 2$)of fourth vector whose (k+n) components $V_i^{(y)}$ ($1 \leq I \leq k+n$, $1 \leq y \leq L$) are respectively set such that $V_i^{(y)} = d^{(y)}/d_i^{(y)} \cdot v_i^{(y)}$ (where $d^{(y)} = d_1^{(y)} d_2^{(y)} \ldots d_{k+n}^{(y)}$) in each set by using L sets of integers $d_i^{(y)}$ and random numbers $v_i^{(y)}$" is met on column 2, lines 38-52; column 10, lines 36-67; column 11, lines 1-11.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have a fourth vector with a second variable of y so as to include an additional factor into the cryptographic system. This is the equivalent of extending a two-dimensional graph to a three dimensional one by adding on a z-axis so as to further detail the specification.

With respect to Claim 15, the limitation of "creating a fourth vector having K (= k+n+h) components by adding together a first vector having k components obtained by dividing a plaintext to be encrypted, a second vector whose components are n arbitrarily selected random numbers and a third vector having h components indicating information identifying positions of

said k components or said n components and obtaining a ciphertext by using the created fourth vector and a publicized fifth vector" is met on column 11, lines 14-67 and on column 12, lines 1-8.

It would have been obvious to one of ordinary skill in the art at the time of the invention to have a fourth vector having k+n+h components by adding a first vector having k components obtained by dividing plaintext to be encrypted because this is analogous to dividing the plaintext into K parts on column 2, lines 38-46.

With respect to Claim 16, the limitation of "wherein the ciphertext is composed of a plurality of blocks obtained by using said fourth vector and ,said fifth vector, and positions of said h components in said fourth vector are identical in each block" is met on column 12, lines 1-11. The ciphertext c is composed of base vector c' and message vector, m'. The base vector, c' represents the fourth vector and the message vector, m' represents the fifth vector. The ciphertext, C is composed of the base vector c' and the message vector, m'.

With respect to Claim 17, the limitation of "wherein the ciphertext is composed of a plurality of blocks obtained by using said fourth vector and said fifth vector, and positions of said k components or said n components in said fourth vector in each block are decided according to said k components in the previous block" is met on column 11, lines 15-67; column 12, lines 1-8.

With respect to Claim 18, the limitation of "wherein the ciphertext is composed of one block obtained by using said fourth vector and said fifth vector and a plurality of blocks obtained by using said fifth vector and said fourth vector in which h components of said third vector are substituted with h components obtained by dividing a plaintext, and positions of (k+h) components or said n components in said fourth vector in each block are decided according to said k or (k+h) components obtained by dividing the plaintext in the previous block" is met on column 11, lines 15-67; column 12, lines 1-8 and on column 13, lines 9-12.

With respect to Claim 19, the limitation of "wherein said fifth vector is generated using a sixth vector whose components Di ($1 \leq i \leq K$) are respectively set such that $Di = (d/di)$ (where d $= d1d2...d_K$) by using an. integer di" is met on column 13, lines 9-18.

With respect to Claims 20, 23, 25, 29 the limitation of "wherein the ciphertext is obtained based on a product-sum operation of the components of said fourth vector and components of said fifth vector modulo -transformed based on said sixth vector" is met on column 13, lines 9-18.

With respect to Claim 21, the limitation of "wherein said fifth vector is generated using a sixth vector whose components Vi ($1 \leq i \leq K$) are respectively set such that $Vi = (d/di).vi$ (where $d = d1d2...dK$) by using an integer di and random number vi" is met on column 13, lines 9-18.

With respect to Claim 24, the limitation of "wherein said fifth vector is generated using L

sets $(L \geq 2)$ of sixth vector whose K components $Di(y)$ $(1 \leq i \leq K,\ 1 \leq y \leq L)$ are respectively set

such that $Di^{(y)} = d^{(y)}/di^{(y)}$ (where $d^{(y)} = d_1^{(y)}d_2^{(y)}\ldots d_K^{(y)}$) in each set by using L sets of integers

$di^{(y)}$" is met on column 13, lines 9-18.

With respect to Claim 26, the limitation of "wherein said fifth vector is generated using L

sets $(L \geq 2)$ of sixth vector whose K components $Vi^{(y)}$ $(1 \leq i \leq k+n,\ 1 \leq y \leq L)$ are respectively set

such that $Vi^{(y)} = d^{(y)}/di^{(y)} \cdot v_i^{(y)}$ (where $d^{(y)} = d_1^{(y)}d_2^{(y)}\ldots d_K^{(y)}$) in each set by using L sets of integers

$di^{(y)}$ and random numbers $v_i^{(y)}$" is met on column 13, lines 9-18; column 11, lines 14-67 and

column 12, lines 1-8.

With respect to Claim 30, the limitation of "wherein the components of said plaintext

vector are decrypted independently of the components of said random number vector" is met on

column 7, lines 1-45.

With respect to Claim 31, the limitation of "wherein the ciphertext is decrypted into the

plaintext while identifying positions of the components of said plaintext vector" is met on

column 7, lines 1-45.

With respect to Claim 32, the limitation of "wherein the ciphertext is decrypted into the

plaintext while identifying positions of the components of said first vector" is met on column 7,

lines 17-20, 6-16.

With respect to Claim 33, the limitation of "creating a ciphertext from a plaintext at a first entity, according to the encryption method of claim 1, and transmitting the ciphertext to a second entity and decrypting the transmitted ciphertext into the plaintext at the second entity" is met on column 3, lines 6-39; and "wherein positions of the components of said plaintext vector or the components of said random number vector in said composite vector are set at the first entity, and information indicating the set positions is sent to the second entity" is met on column 2, lines 38-52.

With respect to Claim 34, the limitation of "the information indicating the set positions is included in a ciphertext to be created, and the ciphertext including the information is transmitted to the second entity" is met on column 6, lines 28-67.

With respect to Claim 35, the limitation of "creating a ciphertext from a plaintext at a first entity, according to the encryption method of claim 1, and transmitting the ciphertext to a second entity and decrypting the transmitted ciphertext into the plaintext at the second entity" is met on column 3, lines 6-39; and "wherein positions of the components of said plaintext vector or the components of said random number vector in said composite vector are set at the second entity, and information indicating the set positions is sent to the first entity" is met on column 2, lines 38-52.

With respect to Claim 36, the limitation of "an encryptor for creating a ciphertext from a plaintext by using the encryption method of claim 1; a communication channel for transmitting the created ciphertext from a first entity to a second entity and a decryptor for decrypting the transmitted ciphertext into the plaintext" is met on column 3, lines 6-39.

With respect to claim 37, its limitation is similar to Claim 1 limitation. The difference is in a computer memory product having computer readable program code that implements the methods described in Claim 1. Hence the existence of a computer readable program code is obvious.

With respect to Claim 38, its limitation is similar to Claim 1 limitation. The difference is in a computer data signal embodied in a carrier wave that transmits the program that performs the methods of Claim 1. Hence the existence of a computer data signal comprising a code segment is obvious.

Claims 7, 12, 13, 22, 27, 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kasahara et al (6798884 B1) in view of Kasahara et al (6785388 B1).

With respect to Claims 7, 22, all the limitation is met by Kasahara et al '884 except for the following limitation.

The limitation of "wherein $gcd(V_i, d_i) = 1$ is satisfied" is met by Kasahara et al '388 on column 16, lines 12-14.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to combine the teachings of Kasahara et al '388 within the system of Kasahara et al '884 because

the greatest common denominator (gcd) of 1 is obvious because Di is composed of di and dj and

they are relative primes ('884 column 2, lines 38-46). Hence their gcd must be equal to one. (Di

is the equivalent of Vi, both are base vectors)

With respect to Claims 12, 27, all the limitation is met by Kasahara et al '884 except for

the following limitation.

The limitation of "wherein gcd(Vi(y), di(y)) = 1 is satisfied" is met by Kasahara et al

'388 on column 16, lines 12-14.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to combine the teachings of Kasahara et al '388 within the system of Kasahara et al '884 because

the greatest common denominator (gcd) of 1 is obvious because Di is composed of di and dj and

they are relative primes ('884 column 2, lines 38-46). Hence their gcd must be equal to one.

With respect to Claim 13, all the limitation is met by Kasahara et al '884 except for the

following limitation.

The limitation of "wherein gcd(di(y), dj(y)) = 1 (1 ≤ j ≤ k+n) is satisfied" is met on

column 16, lines 12-14.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to combine the teachings of Kasahara et al '388 within the system of Kasahara et al '884 because

the greatest common denominator (gcd) of 1 is obvious because Di is composed of di and dj and

they are relative primes ('884 column 2, lines 38-46). Hence their gcd must be equal to one.

With respect to Claim 28, all the limitation is met by Kasahara et al '884 except for the

following limitation.

The limitation of "wherein gcd(di(y), dj(y)) = 1 ($1 \leq j \leq K$) is satisfied" is met on column

16, lines 12-14.

It would have been obvious to one of ordinary skill in the art at the time of the invention

to combine the teachings of Kasahara et al '388 within the system of Kasahara et al '884 because

the greatest common denominator (gcd) of 1 is obvious because Di is composed of di and dj and

they are relative primes ('884 column 2, lines 38-46). Hence their gcd must be equal to one.
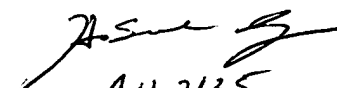

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tracey Akpati whose telephone number is 571-272-3846. The

examiner can normally be reached on 8.30am-6.00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

OTA